Security: It's Just Good Systems Engineering

Ronda R. Henning
Harris Corporation
Rhenning@harris.com

Introduction

- Security engineering is a “black art”
  - A high risk item to cost and schedule
  - Limited skilled personnel
  - Criteria for completion beyond control of customer organization
  - Mission requirements & security requirements conflict

A potential solution

- The Common Criteria for IT Security Evaluation (ISO 15048)
  - Provides a standard notation for requirements
  - Categorizes system security
    - Functional – what the system does
    - Assurance – the lifecycle processes that “assure” a system performs correctly
- Evolving case law from COTS product use
  - National Information Assurance Partnership
  - Common Criteria Interpretations

Assurance

- Grounds for confidence that an entity meets

its security objectives”

- Evaluation Assurance Level (EAL)
  - Defines specific criteria for each category
  - Higher the category, greater the formalism
- Assessment done by a third party

Assurance Requirements

- Categorized in 7 areas:
  1. Configuration Management
  2. Delivery and Operation
  3. Development Correspondence
  4. User Guidance
  5. Lifecycle Support
  6. Testing
  7. Vulnerability Assessment

In Perspective

- The CMMI
  - Integrated guidance on product and process development activities
  - Integrated content from varied disciplines
  - Process framework areas are:
    - Project Management
    - Support
    - Engineering
    - Process Management

More Perspective

- iCMM – FAA variant CMM
- Process Categories
  - Management
  - Life Cycle
  - Support

- A trend: supporting processes that are designed to improve relative quality of a system in operational use.

A Correspondence Exercise

FAA-iCMM v2.0 Process Area	CMMI-SE/SW/IPPD*/A** Process Area	Common Criteria Assurance Class/Family
PA 00 Integrated Enterprise Management	• *Organizational Environment for Integration • Organizational Process Performance	
PA 01 Needs	• Requirements Development	• Functional Specification (ADV_FSP)
PA 02 Requirements	• Requirements Development Requirements Management	Representation Correspondence (ADV_RCR)

A Correspondence Exercise

FAA-iCMM v2.0 Process Area	CMMI-SE/SW/IPPD*/A** Process Area	Common Criteria Assurance Class/Family
PA 03 Design	• Technical Solution	• High-level Design (ADV_HLD) • Security Policy Modeling (ADV_SPM)
PA 06 Design Implementation	• Technical Solution	• Implementation Representation (ADV_IMP) • TSF Internals (ADV_INT) • Low Level Design (ADV_LLD)

Summary of Correspondence

- All Common Criteria Assurance Class families have a home in the CCMI/iCMM process areas
- Common Criteria emphasizes:
  - Correctness in Implementation Correspondence
  - Test Coverage
  - Configuration Management

A Caveat

- Risk is “different”
  - Normally defined as impediments to achievement from perspective of mission functionality vs. cost or schedule
- In Security Parlance
  - Risk is the probability of compromise or exploitation of a vulnerability
- Compromise could be considered an impediment to achievement of mission

Significance

- Security DOES map to process improvement activities that are defined and in place without major distortion
- Need to integrate the security practices with the Maturity Model Practices
  - Example: Configuration Management Processes need to include security configuration information and patch management

Significance

- Security can be an integrated process
- Use of existing process improvement frameworks facilitates that integration
- Result: Organizations follow good security practices without knowing it!

A Caveat

- Do not rush out and say:
  - Because we are a CMMI Level X, we routinely work at Common Criteria Evaluation Assurance Level Y
  - There are security extensions that have to be

    incorporated.
  - A good organizational process helps, but needs adaptation.

Conclusion

- Existing Maturity Model Process Areas accommodate all assurance requirements as defined in the Common Criteria
- Best practices for security could easily be extended into an organization's maturity model framework
- Mitigate risk, reduce security cost, improve discipline integration
- Make security a defined, repeatable activity.